Exercice 1

Montrons que l'ensemble P des nombres premiers est infini.
Supposons que P soit fini, $P = \{p_1, p_2, ..., p_n\}$ ; et notons $M = p_1 p_2 ... p_n + 1$. $M \geq 2$ admet un diviseur premier, supposons que ce soit $p_1$ ; alors $p_1$ divise $M - p_1 p_2 ... p_n = 1$, ce qui amène $p_1 = 1$, ce qui est absurde.

Exercice 2

Soit a et b deux entiers naturels non nuls tels que $PGCD(a + b, ab) = p$ où p est premier.

1. p divise (a + b)a et p divise ab, donc p divise (a + b)a – ab = $a^2$.
2. p divise $a^2$, donc p divise $a^2 = a \times a$. Or p est premier, donc p divise a.

On montre de même que p divise b.

3. Soit D = PGCD(a, b), donc, d'après 2, p divise D.

D divise a et b, donc D divise a + b et ab, d'où D divise $PGCD(a + b, ab) = p$.
p divise D et D divise p, donc p = D.

Exercice 3

1. p est premier et différent de 2, donc PGCD(p, 2) = 1, d'où PGCD(p, 4) = 1. Par le petit théorème de Fermat, $4^{p-1} \equiv 1[p]$. Il existe bien $n = p - 1 \geq 2$ tel que $4^n \equiv 1[p]$.

2. Soit n un entier $\geq 1$ tel que $4^n \equiv 1[p]$ et b le plus petit entier strictement positif tel que $4^b \equiv 1[p]$. $n = bq + r$ où q et r sont des entiers naturels tels que $0 \leq r < b$.

a. $4^b \equiv 1[p]$, donc $(4^b)^q \equiv 1[p]$, soit $4^{bq} \equiv 1[p]$ ; d'où $4^{bq+r} \equiv 4^r [p]$, ce qui amène $4^r \equiv 1[p]$.
Or b le plus petit entier strictement positif tel que $4^b \equiv 1[p]$, donc r = 0. On en déduit que b divise n.

b. Si $4^n \equiv 1[p]$, alors, d'après a, b divise n.

Réciproquement, si b divise n, $n = bq$. $4^b \equiv 1[p]$, donc $(4^b)^q \equiv 1[p]$, soit $4^n \equiv 1[p]$.

c. D'après 1, $4^{p-1} \equiv 1[p]$ ; donc, d'après 2b, b divise p – 1.